TD P 15-71

Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems

March 2002

Reference Number: 2002-20-057

TD P 15-71

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

March 1, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems (Audit # 200120035)

This report presents the results of our review to determine whether taxpayer data was adequately protected from disclosure and alteration from external attacks. Prior Office of Audit reviews, such as *Controls Over the Internet Gateway Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2001-20-101, dated June 2001), have identified significant weaknesses at Internet gateways. To augment those reviews, we contracted with Xacta Corporation to attempt to penetrate the Internal Revenue Service (IRS) network in a manner similar to a hacker.

The IRS is responsible for maintaining the privacy of tax information for over 130 million taxpayers. The IRS has about 100,000 employees located in offices throughout the United States. Most are connected via a wide area network and many IRS employees have access to the Internet. The IRS uses a wide variety of hardware and software to support this system, making security administration difficult.

The likelihood of an external attack has increased significantly in recent years, primarily due to widespread use of the Internet and the interconnectivity of computer systems. As the nation's primary revenue collector, the IRS could be a highly visible target for both foreign and domestic terrorists. To enhance security, we believe it is critical that the IRS understands the techniques of those who could benefit by unlawfully accessing taxpayer information.

In summary, the contractor was able to identify some but not all IRS Internet gateways using publicly available information such as the IRS web site and other web sites commonly known to hackers. While these gateways provide possible entry points for

hackers, the IRS had sound business reasons for publicizing the sites. We believe the risk of advertising these gateways was acceptable considering the business benefits.

The contractor then attempted to penetrate the firewalls at each of the Internet gateways it had identified. In each case, it was unsuccessful. While these results should give the IRS some assurance that the firewalls were configured adequately, the results should be considered with caution. New vulnerabilities are identified frequently and publicized throughout the hacker community. This review was only a snapshot of the IRS' security at a particular time. The contractor had a very limited time to identify and penetrate the firewalls, and consequently used techniques that were more easily identifiable. A persistent hacker could take more time and use less noticeable techniques. In addition, the IRS was aware that the test was taking place and may have been more alert for potential penetration attempts.

Although the contractor could not penetrate the firewalls, it was able to gain sufficient information from employees that could have been used to circumvent the firewalls. The contractor's staff, posing as Help Desk employees, called 100 IRS employees and stated they needed assistance to resolve a network problem. They asked each employee to temporarily change his/her password to one specified by the contractor. Of the 100 employees contacted, 71 agreed to change their password. The contractor was also able to obtain a telephone number enabling it to dial into the IRS network. Armed with passwords, the contractor (or a hacker) could have accessed the network.

The extremely high percentage of employees willing to compromise their passwords indicates that the IRS has not done enough to train employees on their security obligations. Even the best security procedures and controls at Internet gateways can easily be circumvented if employees are not aware of their security responsibilities.

The contractor then worked with the IRS and the Office of Audit to determine the level of access it (or hackers) could have if the firewall had been penetrated or bypassed using information obtained from employees. It conducted vulnerability scans of 110 systems and found that some workstations were configured to allow administrator privileges for anyone using the computer, many had guest accounts enabled, security patches for well-known vulnerabilities had not been updated, and unneeded and exploitable services were running. None of the systems were protected by internal firewalls. If a hacker had penetrated the IRS network, or if a disgruntled employee wanted to disrupt operations, they could have quickly and quietly compromised many of the systems the contractor examined.

The contractor made recommendations to enhance employee awareness of security risks by sending periodic alerts on protecting passwords and on recognizing hacker techniques. The contractor also made technical recommendations, including disabling unnecessary and unused services, and installing up-to-date patches to address known vulnerabilities.

The contractor's report is included as Attachment I.

Management's Response: Management agreed with the recommendations presented. They will coordinate with the Security Program Office and the Computer Security Incident Response group to ensure that employees receive training on preventing computer intrusion and unauthorized access. The Security Program office will continue to raise awareness by communicating to employees the standards regarding password protection. All Information Technology Services system banners will be reviewed for appropriate configuration and be replaced if necessary. Existing practices and procedures will be reviewed by those responsible for system installation and maintenance to ensure the approved banners are implemented on all systems. Any outdated or insecure services will be either disabled or removed from all systems, and an ongoing assessment of these services will be initiated. A memorandum requiring adherence to established procedures and guidelines will be issued.

Management's complete response to the draft report is included as Attachment II.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA's Office of Chief Counsel.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Scott Wilson, Assistant Inspector General for Audit (Information Systems Programs) at (202) 622-8510.

Attachments (2)

cc: Director, Office of Security M:S
Chief, Information Technology Services M:I
Deputy Chief Financial Officer, Department of the Treasury

Attachment I

Copy of XACTA Corporation's PowerPoint Report

"XACTA Network
Penetration Report.p|

Network Penetration Study of the Internal Revenue Service

Network Penetration Study Results

Background

- The Internal Revenue Service (IRS) must maintain the privacy of tax information for over 130 million taxpayers.
- The IRS has about 100,000 employees located in offices throughout the United States. Most are connected via a wide area network and many IRS employees have access to the Internet.
- The IRS uses a wide variety of hardware and software to support this system, making security administration difficult.

TD P 15-71

XACTA™

Background

- The likelihood of an external attack has increased significantly in recent years, primarily due to widespread use of the Internet and the interconnectivity of computer systems.
- The IRS could be a highly visible target for both foreign and domestic terrorists.
- To enhance security, it is critical that the IRS understands the techniques of those who could benefit by unlawfully accessing taxpayer information.

Background

- This penetration study was a "snapshot" in time of the IRS' network security.
- The test was conducted between June and August 2001. The review was performed in accordance with the President's Council on Integrity and Efficiency *Quality Standards for Inspections.*
- No vulnerability test can precisely imitate a bona fide hostile attack since a dedicated malicious attacker will not have time or system restrictions.
- The results of this study are not a replacement for prudent security measures, but should be used to support risk management decisions that strengthen the IRS' overall security posture.

TD P 15-71

XACTA

Scope of Review

- **Xacta provided a penetration study of the IRS computer network.**
  - The study attempted to access IRS data and applications through the Internet and the Local Area Network (LAN) of a large IRS office.
  - The study provided testing that simulates the attack of a hacker using industry standard tools and techniques.
  - Internet testing sought to identify weaknesses in firewall, web server, router, and e-mail controls.
  - LAN testing attempted to access network devices and network services.
  - Techniques, such as pretending to be system administrators and asking for passwords, were used.
  - Treasury Inspector General Tax Administration (TIGTA) auditors were present during all testing.

Scope Of Review (2)

- Although vulnerability scans were performed during the study, scans were not the sole resources used to evaluate the state of network security.
- This study checked the IRS' susceptibility to well-known and publicized vulnerabilities.
- In addition, this assessment sought to identify other possible vulnerabilities using techniques and tools readily available on the Internet.

Methodology

- **Xacta performed this vulnerability assessment in discrete phases:**
  - Phase I – Network Mapping
  - Phase II – External Network Probing
  - Phase III – Internal Host Probing
- **Xacta simulated a malicious outsider attempting to gain access to internal IRS information.**
- **The Xacta team met with TIGTA and IRS personnel at the end of each Phase in order to verify the validity and relevance of the information gathered and to coordinate further activities.**

Methodology - Phase I

- **Xacta accessed publicly available Internet sources and attempted to:**
  - Equate Internet addresses to machine names.
  - Gather valid user names, e-mail addresses and telephone numbers.
  - Piece together a basic target network diagram. Information gathered was available from resources on the Internet, or from the target systems themselves.

TD P 15-71

Methodology - Phase II

- **These tests were conducted to penetrate the firewall:**
  - Port Scans
  - Vulnerability Scans
  - War Dialing (calling telephone numbers to identify dial-in access points to the network). TIGTA provided all telephone numbers used in war dialing.

Methodology - Phase II

- **These tests were conducted to bypass the firewall:**
  - Pretended to work on the “Help Desk”.
  - Calls were made from the “Help Desk” to 100 employees.
  - Asked each to change their password to one predetermined by Xacta.

TD P 15-71

XACTA™

Methodology - Phase III

- Since roughly half of all computer security incidents are traced to the actions of insiders, either inadvertently or accidentally, the rigidity of the inside network security posture was tested.
- The testing performed by Xacta consisted of vulnerability scans of over 100 systems, and was not an all-encompassing scan of every IRS system, but rather a representative sampling.
- The results from the approximately 110 systems that were scanned were analyzed for trends representative of the IRS network as a whole.
- All testing was performed at the IRS New Carrollton facility in the presence of IRS government or contractor personnel.

TD P 15-71

XACTA

Results - Phase I

- **IRS external network security posture:**
  - Information gathered from IRS web pages, using a variety of searches, lookups and web search engines.
  - No obvious security problems discovered based on information gathering.

TD P 15-71

Results - Phase II

- **Xacta was unable to penetrate the firewalls tested.**
  - Provides some assurance that firewalls were configured adequately during the test.
- **Xacta was able to gather information from employees which could have been used to bypass the firewalls.**
  - Convinced 71 of 100 employees to change their passwords.
  - Indicates that the IRS has not adequately trained its employees regarding their security obligations.

TD P 15-71

XACTA

Results - Phase III

- **Systems were not protected by internal firewalls.**
- **Configurations were inconsistent.**
  - Some workstations allowed administrator privileges to anyone using the computer.
  - Many Guest accounts enabled - No user authentication.
  - Outdated and/or misconfigured service packs and patches (see next slide for details).
  - Missing hot fixes (interim vulnerability solution pending official issuance of service pack).
  - Some servers have directories that are accessible by everyone.

TD P 15-71

XACTA™

Results - Phase III

- **Outdated/insecure services were running:**

(b)(7)(E)

TD P 15-71

XACTA™

Recommendations

1. Training on hacker techniques should be given to employees.
2. Alerts and announcements should be periodically issued to advise employees not to divulge log-ons or passwords to anyone.
3. Banners should be configured to not return any operating system or service information.
4. Banners should identify the computer as an official government computer, complete with an "Official Use Only" warning.
5. All unnecessary and unused services should be disabled. Although unnecessary and unused services may not now be vulnerable, they may become so in the future.
6. All operating systems should be updated to the latest Service Packs and patches where possible.
7. All web servers should be patched and upgraded on an ongoing basis.

Attachment II

Management's Response to the Draft Report

DEPUTY COMMISSIONER

LIMITED OFFICIAL USE
DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

FEB - 8 2002

RECEIVED
FEB 1 1 2002

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: John C. Reece
Deputy Commissioner for Modernization &
Chief Information Officer

SUBJECT: Response to Draft Report – Management Advisory Report:
Network Penetration Study of Internal Revenue Service Systems
(Audit # 200120035)

Thank you for the opportunity to review and comment on your draft report and recommendations concerning our network security.

It is our management goal to continually strive for an enhanced security program that effectively manages risks and we appreciate your comments that will further assist us in strengthening our security controls. Attached is a detailed response to each of your recommendations.

If you have any questions or concerns, please feel free to contact me at (202) 622-6800 or Mr. Len Baptiste, Director, Office of Security at (202) 622-8910.

Attachment

Response to Draft Management Advisory Report – Network Penetration Study of Internal Revenue Service Systems (Audit #200120035)

RECOMMENDATION #1:

Training on hacker techniques should be given to employees.

ASSESSMENT OF CAUSE:

Employees are not adequately informed of preventive measures.

CORRECTIVE ACTION(S) TO RECOMMENDATION #1:

The Security Program Office will work with Computer Security Incident Response to ensure that the security awareness program includes training on preventing computer intrusion and unauthorized access.

IMPLEMENTATION DATE(S):

Action	Proposed Completion
Complete Training	January 1, 2003

RESPONSIBLE OFFICIAL(S):

Director, Cyber Security

RECOMMENDATION #2:

Alerts and announcements should be periodically issued to advise employees not to divulge log-ons or passwords to anyone.

ASSESSMENT OF CAUSE:

Employees are not adequately informed of preventive measures.

CORRECTIVE ACTION(S) TO RECOMMENDATION #2:

a) The Security Program Office will continue to use existing media to communicate IRS security standards regarding password procedures and protecting passwords.
b) The Security Program Office will ensure that password protection is incorporated into the required annual security awareness training.
c) The Security Program Office will re-emphasize employee responsibility regarding password protection during the annual Security Awareness Week.

IMPLEMENTATION DATE(S):

Action	Proposed Completion
a) Disseminate Information	July 1, 2002
b) Complete Training	January 1, 2003
c) Complete Activity	January 1, 2003

RESPONSIBLE OFFICIAL(S):

Director, Office of Cyber Security

RECOMMENDATION #3:

Banners should be configured to not return any operating system or service information.

ASSESSMENT OF CAUSE:

Banners may be bundled with operating system packages.

CORRECTIVE ACTION (S) TO RECOMMENDATION #3:

The officials responsible for the installation and implementation of operating systems will review all Information Technology Services (ITS) system banners for appropriate configuration and initiate replacement as required.

IMPLEMENTATION DATE(S):

Action	Proposed Completion
Review ITS Systems	August 2002
Repair Systems	November 2002

RESPONSIBLE OFFICIAL(S):

Director, End User Equipment and Services
Director, Enterprise Operations

RECOMMENDATION #4:

Banners should identify the computer as an official government computer, complete with an "Official Use Only" warning.

ASSESSMENT OF CAUSE:

Standard configuration of the Microsoft NT Operating System does not place a banner on workstations or servers.

CORRECTIVE ACTION(S) TO RECOMMENDATION #4:

The official responsible for the installation and maintenance of ITS computer systems will review existing practices and procedures to ensure the approved standard banner mandated by the Law Enforcement Manual, Chapter 6.3.8 is properly implemented on all ITS systems.

IMPLEMENTATION DATE(S):

Action	Proposed Completion
Review Practices and Procedures	August 2002
Repair Systems	November 2002

RESPONSIBLE OFFICIAL(S):

Director, End User Equipment and Services

RECOMMENDATION #5:

All unnecessary and unused services should be disabled. Although unnecessary and unused services may not now be vulnerable, they may become so in the future.

ASSESSMENT OF CAUSE:

System commands are bundled with operating systems.

CORRECTIVE ACTION (S) TO RECOMMENDATION #5:

Any identified outdated/insecure services will be reviewed and a determination made for either disabling or removing using automated processes and tools. A process will be developed and implemented for continued assessment of the existence of unnecessary and unused services on ITS systems.

IMPLEMENTATION DATE (S):

Action	Proposed Completion
Review	August 2002
Disable/Remove Services	November 2002
Develop Assessment Process	December 2002

RESPONSIBLE OFFICIAL (S):

Director, End User Equipment and Services
Director, Enterprise Operations

RECOMMENDATION #6:

All operating systems should be updated to the latest Service Packs and patches where possible.

ASSESSMENT OF CAUSE:

Inconsistencies exist in the application of Service Packs and patches.

CORRECTIVE ACTION (S) TO RECOMMENDATION #6:

The responsible officials will issue a memorandum requiring adherence to established procedures and guidelines that provide the standards for enterprise-wide updates of Service Packs and patches. A date for compliance will be included in the memorandum. Automated processes will be initiated to ensure these standards are being followed and systemic updates will be implemented appropriately.

IMPLEMENTATION DATE(S):

Action	Proposed Completion
Prepare Memorandum	June 2002
Implement Automated Review Process	November 2002

RESPONSIBLE OFFICIAL(S):

Director, End User Equipment and Services
Director, Enterprise Operations
Director, Web Services

RECOMMENDATION #7

All web servers should be patched and upgraded on an ongoing basis.

ASSESSMENT OF CAUSE:

Inconsistencies exist in the application of Service Packs and patches.

CORRECTIVE ACTION(S) TO RECOMMENDATION #7:

The responsible official will issue a memorandum requiring MITS adherence to established procedures and guidelines that provide the standards for enterprise-wide updates of Service Packs and patches which will include web servers. (See corrective action for Recommendation # 6.)

IMPLEMENTATION DATE(S):

Action	Proposed Completion
Prepare Memorandum	June 2002

RESPONSIBLE OFFICIAL(S):

Director, Web Services